EVIL PRIMES AND SUPERSPECIAL MODULI

EYAL Z. GOREN & KRISTIN E. LAUTER

Abstract. For a quartic primitive CM field K, we say that a rational prime p is *evil* if at least one of the abelian varieties with CM by K reduces modulo a prime ideal $\mathfrak{p}|p$ to a product of supersingular elliptic curves with the product polarization. We call such primes *evil primes for* K. In [GL], we showed that for fixed K, such primes are bounded by a quantity related to the discriminant of the field K. In this paper, we show that evil primes are ubiquitous in the sense that, for any rational prime p, there are an infinite number of fields K for which p is evil for K. The proof consists of two parts: (1) showing the surjectivity of the abelian varieties with CM by K, for K satisfying some conditions, onto the the superspecial points modulo $\mathfrak{p}$ of the Hilbert modular variety associated to the intermediate real quadratic field of K, and (2) showing the surjectivity of the superspecial points modulo $\mathfrak{p}$ of the Hilbert modular variety associated to a large enough real quadratic field onto the superspecial points modulo $\mathfrak{p}$ with principal polarization on the Siegel moduli space.

1. Introduction

Given a primitive quartic CM field, K, one can study the values at CM points associated to K of certain Siegel modular functions studied by Igusa. Their values are algebraic numbers which generate unramified abelian extensions of the reflex field of K. When computing their minimal polynomials over $\mathbb{Q}$, rational primes in the denominators of the coefficients correspond to primes where at least one of the abelian varieties with CM by K reduces to a product of supersingular elliptic curves with the product polarization. We call such primes *evil primes for* K. Such primes were studied in [GL], where we showed that for fixed K, such primes are bounded by a quantity related to the discriminant of the field K. So in some sense, there are few evil primes, since if we fix K with small discriminant, then there are a small number of evil primes for K. In this paper, we show that evil primes are ubiquitous in the sense that, for any finite set S of rational primes, there are an infinite number of fields K for which every prime $p \in S$ is evil for K (this requires the existence of infinitely many real quadratic fields of strict class number one, but we expect that this condition can be removed). The presence of evil primes appears as an obstruction for the class invariants defined in [DSG] to be units (see also [GL]).

The proof is divided into two parts, corresponding to the two main theorems of the paper, Theorem A and Theorem B. Let L be a totally real number field of strict class number one. In Theorem A we prove that there is a choice of CM field K such that all the superspecial points in characteristic p on the Hilbert modular variety associated to L arise as the reduction of an abelian variety with CM by K. Necessary and sufficient conditions on the field K are: $K^+ = L$, p is unramified in K and satisfies conditions ensuring that any abelian variety with CM by $\mathcal{O}_K$ has superspecial reduction, and the relative discriminant $\mathrm{Norm}(d_{K/L})$ is large enough.

Theorem A generalizes recent work of Elkies, Ono and Yang [EOY], where they study the elliptic curve case corresponding to an imaginary quadratic field K. In Theorem 1.2 of [EOY], they prove that for an odd prime p and an imaginary quadratic field K in which p is inert, (any power of) the supersingular polynomial modulo p divides the Hilbert class polynomial of K modulo p if the discriminant of K is large enough. In other words, any supersingular elliptic curve modulo p is the reduction of an elliptic curve with CM by K for any K satisfying the above conditions. Whereas Theorem 1.2 of [EOY] uses deep results of Duke [D], Iwaniec [I], and Siegel to study the asymptotics of a certain theta function, our Theorem A uses the work of Cogdell, Piatetski-Shapiro and Sarnak [Cog] which generalizes Duke's work

1991 *Mathematics Subject Classification.* Primary 11G15, 11G16 Secondary 11G18, 11R27.

to totally real number fields. We prove Theorem A in three steps. Let R be the centralizer of $\mathcal{O}_L$ in the endomorphism ring of A, a superspecial point on the reduction modulo a prime above p of the Hilbert modular variety associated to L. Following [Nic], we call R a superspecial order; it is an order in the quaternion algebra $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$, where $B_{p,\infty}$ is the rational quaternion algebra ramified at p and ∞ alone. First we establish a one-to-one correspondence between $\mathcal{O}_L$-embeddings of $\mathcal{O}_K$ into the order R up to equivalence and CM lifts of A to abelian varieties with CM by K along the lines of what was shown in [GL]. Next we show that to give an $\mathcal{O}_L$-embedding of $\mathcal{O}_K$ into the endomorphism ring of A, it is enough that a totally positive generator of the relative discriminant of K/L be represented by the norm form on a lattice associated to R. Next we use the theorem on integral representability by positive definite integral ternary quadratic forms over totally real fields ([Cog]) to reduce the computation to checking local representability. Checking local representability uses that all superspecial orders in the quaternion algebra $B_{p,L}$ are locally conjugate.

Theorem B concerns the relationship between the superspecial points modulo a prime on the Siegel moduli space of principally polarized abelian surfaces and the superspecial points modulo a prime on the Hilbert modular variety associated to a real quadratic field L. Specifically, in Theorem B we show that the superspecial points modulo a prime on the Hilbert modular variety associated to a real quadratic field L surject onto the superspecial points modulo the prime on the Siegel moduli space if the discriminant of L is large enough. To prove this theorem we need to show how to embed $\mathcal{O}_L$ into the endomorphism ring of A, for A any superspecial point with principal polarization, in a way which is compatible with the polarization. We accomplish this using the description of all possible polarizations given in [IKO] and the fact that locally and rationally all principally polarized abelian varieties are the same.

Together Theorems A and B imply that for any rational prime p, there are an infinite number of quartic CM fields K for which p is evil for K. Moreover, once the discriminants of K and its totally real subfield L are large enough, every reducible polarized abelian surface $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ arises as the reduction of a CM point of K. Strictly speaking, the second statement requires that L have strict class number one. It is widely believed that there are infinitely many real quadratic fields of strict class number one, and in any case we expect that the strict class number one assumption can be removed. Note that the first statement is unconditional, however, since one can easily manufacture a reducible $\mathcal{O}_L$-principally polarized surface and then use Theorem A. The analogous statement for any finite collection of primes still requires the existence of infinitely many real quadratic fields of strict class number one, since all primes in the set must be unramified in the real quadratic field.

We also remark that Theorems A and B could be of interest for totally different reasons. In [Ghi, Nic], one finds an approach to Siegel and Hilbert modular forms through the superspecial locus in the corresponding moduli spaces.

The paper is organized as follows. Section 2 contains precise statements of the results of the paper. Section 3 contains the proof of Theorem A and Section 4 contains the proof of Theorem B.

2. Statement of Results

All fields are considered as subfields of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Given a CM field K of degree $2g$ over $\mathbb{Q}$, denote by $\mathscr{S}(K)$ the set of isomorphism classes over $\overline{\mathbb{Q}}$ of abelian varieties (A, λ, ι), where A is an abelian variety of dimension g, $\lambda : A \longrightarrow A^\vee$ is a principal polarization, $\iota : \mathcal{O}_K \longrightarrow \mathrm{End}(A)$ is a ring embedding and the Rosati involution $x \mapsto x^\lambda$ induces on $\mathcal{O}_K$ complex conjugation. We denote by K^+ the maximal totally real subfield of K. If K^+ has strict class number one then the discriminant ideal d_{K/K^+} is generated by a totally negative element of K^+, uniquely determined up to ${\mathcal{O}_L}^{\times,2}$ (see Lemma 1). We shall denote any such generator as $-m$.

Theorem A. *Let L be a totally real field of degree g and strict class number one. Let p be a rational prime, unramified in L, and P a prime of $\overline{\mathbb{Q}}$ above p. Let $\mathscr{SS}(L)$ denote the superspecial points on the reduction modulo P of the Hilbert modular variety associated to L that parameterizes abelian varieties with*

real multiplication by $\mathcal{O}_L$ equipped with an $\mathcal{O}_L$-linear principal polarization. There exists a constant $N = N(p, L)$ such that for every CM field K satisfying:

(1) $K^+ = L$;
(2) *Let $\mathfrak{p}$ be a prime of L above p and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$.*
   (a) *If $p \neq 2$ then $f(\mathfrak{P}/\mathfrak{p}) + f(\mathfrak{p}/p)$ is odd for all $\mathfrak{P}|\mathfrak{p}|p$;*
   (b) *If $p = 2$ then $3m$ is a quadratic residue modulo $\mathfrak{p}^3$ for all $\mathfrak{p}|p$;*
(3) *the discriminant of K over L, $d_{K/L}$, has norm greater than N in absolute value;*

then the reduction map

$$\mathscr{S}(K) \longrightarrow \mathscr{SS}(L)$$

is surjective.

Theorem B. *Let L be a real quadratic field of strict class number one. Let p be a rational prime. Let $\mathcal{A} = \mathcal{A}_{2,1}$ denote the moduli space of principally polarized abelian surfaces. Let $\mathscr{SS}(\mathcal{A})$ denote the superspecial points of $\mathcal{A}$ (mod p). There exists a constant $M = M(p)$ such that if $d_L > M$ the map*

$$\mathscr{SS}(L) \longrightarrow \mathscr{SS}(\mathcal{A})$$

is surjective.

Corollary 1. *Let L be a real quadratic field of strict class number one and let p be a rational prime unramified in L, and suppose that L satisfies $d_L > M = M(p)$ from Theorem B. If K is a non-biquadratic quartic CM field satisfying conditions (1) - (3) of Theorem A, then every superspecial principally polarized abelian variety in characteristic p has a CM lift to an abelian variety with CM by K, i.e., is a reduction of a point in $\mathscr{S}(K)$.*

Definition. Let K be a quartic primitive CM field. We say that a rational prime is "evil" (for K) if for some prime P of $\overline{\mathbb{Q}}$ there is an element of $\mathscr{S}(K)$ whose reduction modulo P is the product of two supersingular elliptic curves with the product polarization.

Corollary 2. *Let L be a real quadratic field of strict class number one and let p be a rational prime unramified in L, and suppose that L satisfies $d_L > M = M(p)$ from Theorem B. Then p is evil for every non-biquadratic quartic CM field K satisfying conditions (1) -(3) of Theorem A.*

Remark 1. In Corollaries 1 and 2, the rational prime p can be replaced by a finite set of rational primes, all unramified in L. The results of the corollaries then hold for fields Ksatisfying the conditions of Theorem A for all primes in the set simultaneously. In particular, for any finite set of rational primes, this gives a field K for which all primes in the set are evil for K.

3. Proof of Theorem A

Let L be a totally real number field of degree g over $\mathbb{Q}$ and let K be a CM field such that $K^+ = L$. We assume that L has strict class number one.

Lemma 1.
(1) *One can write $\mathcal{O}_K = \mathcal{O}_L[t]$ where t satisfies a quadratic polynomial $x^2 + bx + c$, with $b, c \in \mathcal{O}_L$. Let $-m = b^2 - 4c$. Then $-m$ is a totally negative generator of $d_{K/L}$. We have that $\mathcal{D}_{K/L}^{-1} = \mathcal{O}_K\left[\frac{1}{\sqrt{-m}}\right]$.*
(2) *Let A be an abelian variety with real multiplication by $\mathcal{O}_L$ such that the Rapoport condition holds (cf.* [GL]*). Then A has an $\mathcal{O}_L$-linear principal polarization which is unique up to automorphism.*
(3) *Let Φ be a CM type of K and let $\mathfrak{a}$ be a fractional ideal in K. The abelian variety $\mathbb{C}^g/\Phi(\mathfrak{a})$ carries a principal polarization λ such that the Rosati involution associated to it induces complex conjugation on K. Moreover, λ is unique up to automorphism.*

Proof. Since $\mathcal{O}_L$ has strict class number one, and $\mathcal{O}_K$ is a torsion-free $\mathcal{O}_L$-module, we may write $\mathcal{O}_K = \mathcal{O}_L \oplus \mathcal{O}_L \cdot t$. Then $t^2 = -c - bt$ for some $b, c \in \mathcal{O}_L$. It follows that the discriminant ideal $d_{K/L}$ is generated by $\mathrm{Norm}_{K/L}(2t+b) = \mathrm{Norm}_{K/L}(\sqrt{-m}) = m$ ([Ser, Ch 3, §6, Cor 2]) and that $\mathcal{D}_{K/L}^{-1} \supseteq \mathcal{O}_K\left[\frac{1}{\sqrt{-m}}\right]$. We deduce equality by comparing the norm to L of these ideals. We conclude Part (1).

It is proven in [Rap] that A has an $\mathcal{O}_L$-linear polarization. Since the polarization module of A is a projective $\mathcal{O}_L$-module with a notion of positivity, it follows that there is an isomorphism of $\mathcal{O}_L$-modules $\mathrm{Hom}_{\mathcal{O}_L}(A, A^\vee)^{\mathrm{sym}} \cong \mathcal{O}_L$, taking the polarizations to the totally positive elements. Since A satisfies the Rapoport condition, it can be lifted as a polarized abelian variety with RM to characteristic zero. The characteristic zero uniformization allows us to deduce that the degree of a symmetric homomorphism, viewed as an element $\lambda \in \mathcal{O}_L$, is $\mathrm{Norm}(\lambda)^2$. In particular, principal polarizations exist and are in bijection with ${\mathcal{O}_L}^{\times,+}$.

Now, for any totally real number field L of degree g we have an exact sequence

$$1 \longrightarrow L^\times/(L^{\times,+} \cdot {\mathcal{O}_L}^\times) \longrightarrow \mathrm{Cl}^+(L) \longrightarrow \mathrm{Cl}(L) \longrightarrow 1.$$

There is a sign map, $\mathrm{sgn} : L^\times \longrightarrow \{\pm 1\}^g$, which is a surjective homomorphism with kernel $L^{\times,+}$. Thus, the cardinality of $L^\times/(L^{\times,+} \cdot {\mathcal{O}_L}^\times)$ is $2^g/|\mathrm{sgn}({\mathcal{O}_L}^\times)|$. If we interpret 2^g as the cardinality of ${\mathcal{O}_L}^\times/{\mathcal{O}_L}^{\times,2}$ and $|\mathrm{sgn}({\mathcal{O}_L}^\times)|$ as the cardinality of ${\mathcal{O}_L}^\times/{\mathcal{O}_L}^{\times,+}$ we conclude that $|{\mathcal{O}_L}^{\times,+}/{\mathcal{O}_L}^{\times,2}| = h_L^+/h_L$. In particular, the statement $h_L^+ = 1$ is equivalent to the statement that $h_L = 1$ and ${\mathcal{O}_L}^{\times,+} = {\mathcal{O}_L}^{\times,2}$.

Now let λ_1, λ_2 be two principal $\mathcal{O}_L$-linear polarizations on the abelian variety with real multiplication (A, ι) . We may identify the λ_i with totally positive units in $\mathcal{O}_L$ and so there is a unit $\epsilon \in \mathcal{O}_L$ such that $\lambda_2 = \epsilon^2 \lambda_1$. That implies that the polarized abelian varieties (A, ι, λ_1) and (A, ι, λ_2) are isomorphic via the multiplication by ϵ map.

Next we address Part (3). It is well known that the polarizations on $\mathbb{C}^g/\Phi(\mathfrak{a})$ that induce complex conjugation on K arise from bilinear pairings

$$E_\rho : \mathfrak{a} \times \mathfrak{a} \longrightarrow \mathbb{Z}, \qquad E_\rho(u, v) = \mathrm{Tr}_{K/\mathbb{Q}}(\rho u \bar{v}),$$

where $\rho \in (\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$, $\bar{\rho} = -\rho$, and $\mathrm{Im}(\phi(\rho)) > 0$ for all $\phi \in \Phi$. The polarization is principal if and only if $(\rho) = (\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$.

It follows from Part (1) that $\mathcal{D}_{K/L} = (\sqrt{-m})$ and since L has strict class number one we also have $\mathcal{D}_{L/\mathbb{Q}} = (\eta)$ for some totally positive η. Since $\mathcal{D}_{K/\mathbb{Q}} = \mathcal{D}_{K/L}\mathcal{D}_{L/\mathbb{Q}}$, we conclude that $\mathcal{D}_{K/\mathbb{Q}} = (\delta)$, where $\bar{\delta} = -\delta$. Again, the strict class number one condition gives that $\mathrm{sgn}({\mathcal{O}_L}^\times) = \{\pm 1\}^g$ and so modifying δ by a unit $\epsilon \in {\mathcal{O}_L}^\times$ we can achieve also $\mathrm{Im}(\phi(\delta)) > 0$ for all $\phi \in \Phi$. Given a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ there is an $a \in L^+$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (a)$. Letting $\rho = 1/(\delta a)$, we see that $\mathbb{C}^g/\Phi(\mathfrak{a})$ carries a principal polarization. Moreover, the element ρ is unique up to multiplication by elements of ${\mathcal{O}_L}^{\times,+} = {\mathcal{O}_L}^{\times,2}$ and the same argument as in Part (2) shows that different choices of ρ lead to isomorphic polarized abelian varieties with CM. □

Let $A \in \mathscr{SS}(L)$. There is a given embedding $\iota : \mathcal{O}_L \longrightarrow \mathrm{End}(A)$ and a unique up-to-isomorphism $\mathcal{O}_L$-linear principal polarization for this embedding. The centralizer R of $\mathcal{O}_L$ in $\mathrm{End}(A)$ is an order of the quaternion algebra $B_{p,L} = B_{p,\infty} \otimes L$, where $B_{p,\infty}$ is the quaternion algebra over $\mathbb{Q}$ ramified at p and infinity (cf. [Cha, Lemma 6]). In particular $B_{p,L}$ is ramified at any infinite place of L. It follows that the Rosati involution coming from an $\mathcal{O}_L$-polarization fixes R and induces on it the canonical involution $x \mapsto \bar{x} := \mathrm{Tr}(x) - x$.

The orders R that arise in this way are called superspecial in [Nic]. In his thesis [Nic], Nicole develops a theory analogous to Deuring's theory for supersingular elliptic curves and we refer the reader to that reference for a comprehensive picture (see also [GN]). The only fact that we need here is that if (A_i, ι_i), $i = 1, 2$, are two superspecial abelian varieties with real multiplication by $\mathcal{O}_L$ and $R_i = \mathrm{Cent}_{\mathrm{End}(A_i)}(\mathcal{O}_L)$ then R_1 and R_2 are everywhere locally conjugate. For completeness we sketch the argument.

As is well-known, Tate's theorem for abelian varieties (see for example [WM]) can be simplified for supersingular abelian varieties over a finite field of characteristic p and written as

$$\mathrm{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}(T_\ell(A_1), T_\ell(A_2)), \qquad \mathrm{Hom}(A_1, A_2) \otimes \mathbb{Z}_p \cong \mathrm{Hom}(\mathbb{D}(A_1), \mathbb{D}(A_2)), \tag{3.1}$$

where $\mathbb{D}(A_i)$ is the co-variant Dieudonné module of A_i (the Hom's are over $\overline{\mathbb{F}}_p$). It is not hard to see that if A_i have RM by $\mathcal{O}_L$ then we get

(3.2)

$$\mathrm{Hom}_{\mathcal{O}_L}(A_1,A_2)\otimes\mathbb{Z}_\ell\cong\mathrm{Hom}_{\mathcal{O}_L}(T_\ell(A_1),T_\ell(A_2)),\qquad \mathrm{Hom}_{\mathcal{O}_L}(A_1,A_2)\otimes\mathbb{Z}_p\cong\mathrm{Hom}_{\mathcal{O}_L}(\mathbb{D}(A_1),\mathbb{D}(A_2)).$$

Since $T_\ell(A)\cong(\mathcal{O}_L\otimes\mathbb{Z}_\ell)^2$ and the isomorphism type of the Dieudonné module $\mathbb{D}(A)$ doesn't depend on A if p is unramified (see [GO, Thm 5.4.4]) we conclude that the orders $\mathrm{End}_{\mathcal{O}_L}(A_i)$ are locally isomorphic at any prime.

Given an $\mathcal{O}_L$-embedding of $\mathcal{O}_K$ into R, the action of $\mathcal{O}_K$ will satisfy the Kottwitz condition automatically, because $\mathcal{O}_L$ does by assumption. The Rosati involution defined by any principal $\mathcal{O}_L$-polarization will induce complex conjugation on K. By [GL, Lemma 4.4.1] this gives an element of $\mathscr{S}(K)$ reducing to A.

The problem is thus translated to showing the existence of an embedding of $\mathcal{O}_K$ into such an order R if K satisfies certain conditions. Let R^0 denote the elements of reduced trace 0 in R and let $\Lambda_R=R^0\cap(\mathcal{O}_L+2R)$. This is an $\mathcal{O}_L$-lattice of rank 3 equipped with a positive definite $\mathcal{O}_L$-valued quadratic form N (which is just the restriction of the reduced norm on the quaternion algebra $R\otimes_{\mathcal{O}_L}L$ to Λ_R)

$$N:\Lambda_R\longrightarrow\mathcal{O}_L,\qquad x\mapsto N(x)=x\bar{x}=-x^2.$$

Lemma 2. *Let $-m$ be a totally negative generator of $d_{K/L}$. Then $\mathcal{O}_K\hookrightarrow R$ if and only if m is represented by the ternary quadratic form N on Λ_R.*

Proof. We write $\mathcal{O}_K=\mathcal{O}_L[t]$ where $t^2+bt+c=0$ as in Lemma 1. If $t=(-b+\sqrt{-m})/2$ is in R then $\sqrt{-m}=b+2t\in\Lambda_R$ and its norm is m. Conversely, suppose that there is an element $x\in\Lambda_R$ such that $N(x)=m$. This gives a map $K\longrightarrow B_{p,L}$ taking $\sqrt{-m}$ to x. We may write $x=x_1+2x_2$, where $x_i\in\mathcal{O}_L$, $x_2\in R$, and so the image of the element $\alpha=\frac{-x_1+\sqrt{-m}}{2}$ is in R, hence it is an integral element. That is, $\alpha\in\mathcal{O}_K$. We conclude that $\mathcal{O}_L[\alpha]\subseteq\mathcal{O}_K$. In fact, $\mathcal{O}_L[\alpha]=\mathcal{O}_K$ because $t-\alpha\in L\cap\mathcal{O}_K=\mathcal{O}_L$. Since $\mathcal{O}_L[\alpha]\subset R$, our claim follows. □

We shall use the following theorem of Cogdell, Piatetski-Shapiro and Sarnak [Cog] in the case of strict class number one.

Theorem. *Let $q(x_1,x_2,x_3)$ be a positive definite integral ternary quadratic form over L. Then there is a constant C_q such that if α is a totally positive square-free integer of O_L with $\mathrm{Norm}_{L/\mathbb{Q}}(\alpha)>C_q$ then α is represented integrally by q if and only if it is represented integrally locally over every completion of L, i.e., when $\mathrm{Norm}_{L/\mathbb{Q}}(\alpha)>C_q$ we have $\alpha=q(x_1,x_2,x_3)$ for some $x_i\in\mathcal{O}_L$ if and only if for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ we have $\alpha=q(x_{1,\mathfrak{p}},x_{2,\mathfrak{p}},x_{3,\mathfrak{p}})$ for some $x_{i,\mathfrak{p}}\in\mathcal{O}_{L_\mathfrak{p}}$.*

Using this theorem one reduces to verifying that the norm N on Λ_R represents m locally at every prime $\mathfrak{p}$ of $\mathcal{O}_L$. We note that $\Lambda_R\otimes_{\mathcal{O}_L}\mathcal{O}_{L_\mathfrak{p}}=\Lambda_{R\otimes_{\mathcal{O}_L}\mathcal{O}_{L_\mathfrak{p}}}:=(R\otimes_{\mathcal{O}_L}\mathcal{O}_{L_\mathfrak{p}})^0\cap(\mathcal{O}_{L_\mathfrak{p}}+2R\otimes_{\mathcal{O}_L}\mathcal{O}_{L_\mathfrak{p}})$ (cf. Proposition 3). Since all the orders R that arise are locally isomorphic, the isomorphism leaving the trace and norm unchanged, and the formation of the lattices commutes with completions, it suffices to deal with a single order R, which we now proceed to do.

Let E be a supersingular elliptic curve and $A=E\otimes_{\mathbb{Z}}\mathcal{O}_L$. As an abelian variety A is isomorphic to E^g and its functor of points is canonically given by $A(R)=E(R)\otimes_{\mathbb{Z}}\mathcal{O}_L$. It is thus a superspecial abelian variety with $\mathcal{O}_L$-action and, since it satisfies the Rapoport condition ($T_{E\otimes_{\mathbb{Z}}\mathcal{O}_L,0}=T_{E,0}\otimes_{\mathbb{Z}}\mathcal{O}_L$), it carries a unique principal $\mathcal{O}_L$-linear polarization up to isomorphism, thus giving a point of $\mathscr{SS}(L)$. In this case $R=\mathcal{O}\otimes_{\mathbb{Z}}\mathcal{O}_L$, where $\mathcal{O}\subset B_{p,\infty}$ is a maximal order identified once and for all with $\mathrm{End}(E)$ (see [Nic, Proposition 2.5.26.]). Set $\Lambda_\mathcal{O}=\mathcal{O}^0\cap(\mathbb{Z}+2\mathcal{O})$, where $\mathcal{O}^0$ are the trace zero elements of $\mathcal{O}$. In this case one can prove the following.

Proposition 3. *(i) $\Lambda_R=\Lambda_\mathcal{O}\otimes_{\mathbb{Z}}\mathcal{O}_L$ and the norm form on Λ_R is the extension of scalars of the norm form on $\Lambda_\mathcal{O}$.*

(ii) Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ and $\mathcal{O}_{L_\mathfrak{q}}$ the ring of integers of the completion $L_\mathfrak{q}$ of L at $\mathfrak{q}$. Let $q = \mathfrak{q} \cap \mathbb{Z}$. Then $\Lambda_R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{q}} = \Lambda_\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q \otimes_{\mathbb{Z}_q} \mathcal{O}_{L_\mathfrak{q}}$.

(iii) $\Lambda_\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q = (\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q)^0 \cap (\mathbb{Z}_q + 2\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q)$ (namely, the construction of the lattice $\Lambda_\mathcal{O}$ commutes with localization). Moreover the norm form induced on $\Lambda_\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q$ is none other than the norm form induced from $B_{p,\infty} \otimes_\mathbb{Q} \mathbb{Q}_q$.

Proof. (i) The exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow (\mathbb{Z} + 2\mathcal{O}) \cap \mathcal{O}^0 \longrightarrow \mathcal{O}^0 \longrightarrow \mathcal{O}/(\mathbb{Z} + 2\mathcal{O}) \longrightarrow 0$$

remains exact when tensored with the flat $\mathbb{Z}$-module $\mathcal{O}_L$. So

$$\Lambda_\mathcal{O} \otimes \mathcal{O}_L = ((\mathbb{Z} + 2\mathcal{O}) \cap \mathcal{O}^0) \otimes \mathcal{O}_L = \ker[\mathcal{O}^0 \otimes \mathcal{O}_L \longrightarrow (\mathcal{O} \otimes \mathcal{O}_L)/(\mathcal{O}_L + 2\mathcal{O} \otimes \mathcal{O}_L)]$$
$$= (\mathcal{O}^0 \otimes \mathcal{O}_L) \cap (\mathcal{O}_L + 2\mathcal{O} \otimes \mathcal{O}_L) = R^0 \cap (\mathcal{O}_L + 2R) = \Lambda_R$$

Part (ii) follows from (i).

(iii) The same argument as for (i) works when tensoring the above exact sequence with the flat $\mathbb{Z}$-module $\mathbb{Z}_q$. □

Picking a convenient model for $\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q$, we can now calculate $\Lambda_\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q$ and its norm form explicitly, extend scalars to $\mathcal{O}_{L_\mathfrak{q}}$, and check that there are no local obstructions to representing m. We consider two cases.

Case I: $\mathfrak{q}|q, q \neq p$ Outside of p and ∞, $B_{p,\infty}$ is unramified, so

$$\mathcal{O} \otimes \mathbb{Z}_q \cong M_2(\mathbb{Z}_q),$$

where the reduced trace is the trace of a matrix and the reduced norm is the determinant of a matrix. So

$$(\mathcal{O} \otimes \mathbb{Z}_q)^0 \cong \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a, b, c \in \mathbb{Z}_q \right\},$$

and

$$\mathbb{Z}_q \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_q \right\}.$$

So

$$\Lambda_\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q = (\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q)^0 \cap (\mathbb{Z}_q + 2\mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_q) \cong \left\{ \begin{pmatrix} a & 2b \\ 2c & -a \end{pmatrix} : a, b, c \in \mathbb{Z}_q \right\},$$

and

$$\Lambda_R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{q}} \cong \left\{ \begin{pmatrix} a & 2b \\ 2c & -a \end{pmatrix} : a, b, c \in \mathcal{O}_{L_\mathfrak{q}} \right\}.$$

The question of whether m is represented locally at $\mathfrak{q}$ is now a question of whether $m = -a^2 - 4bc$, which is obviously the case.

Case II: $\mathfrak{q}|p$ Let $\mathbb{Q}_{p^2}$ be the unramified extension of degree two of $\mathbb{Q}_p$ and $\mathbb{Z}_{p^2}$ its maximal order. In this case, we can verify using [Vig, Ch. II, Théorème 1.1] that

$$B_{p,\infty} \otimes \mathbb{Q}_p = \left\{ \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix} : a, b \in \mathbb{Q}_{p^2}, \sigma = \text{Frobenius} \right\}.$$

This is a division algebra over $\mathbb{Q}_p$, whose trace and norm are in this model the trace and determinant of matrices. The algebra $B_{p,\infty} \otimes \mathbb{Q}_p$ has a unique maximal order consisting of all the elements with integral norm [Vig, Ch. II, Lemme 1.5]. Therefore, the maximal order is

$$\mathcal{O} \otimes \mathbb{Z}_p = \left\{ \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\},$$

and

$$(\mathcal{O}\otimes\mathbb{Z}_p)^0=\left\{\begin{pmatrix}a & b\\ -pb^\sigma & a^\sigma\end{pmatrix} : a+a^\sigma=0, a,b\in\mathbb{Z}_{p^2}\right\}.$$

So

$$\begin{aligned}\Lambda_{\mathcal{O}}\otimes\mathbb{Z}_p &= (\mathcal{O}\otimes\mathbb{Z}_p)^0\cap(\mathbb{Z}_p+2\mathcal{O}\otimes\mathbb{Z}_p)\\ &=\left\{\begin{pmatrix}a+2\alpha & 2\beta\\ -2p\beta^\sigma & a+2\alpha^\sigma\end{pmatrix} : a+\alpha+\alpha^\sigma=0, a\in\mathbb{Z}_p,\alpha,\beta\in\mathbb{Z}_{p^2}\right\}\\ &=\left\{\begin{pmatrix}\alpha-\alpha^\sigma & 2\beta\\ -2p\beta^\sigma & \alpha^\sigma-\alpha\end{pmatrix} : \alpha,\beta\in\mathbb{Z}_{p^2}\right\}.\end{aligned}\tag{3.3}$$

From this point we proceed by considering two possibilities.

Case II a: $p\neq 2$ Write $\mathbb{Z}_{p^2}=\mathbb{Z}_p+\sqrt{r}\mathbb{Z}_p$, where r is not a square modulo p. Then we can write down the following $\mathbb{Z}_p$-basis for the above collection of matrices:

$$e_1=\begin{pmatrix}\sqrt{r} & 0\\ 0 & -\sqrt{r}\end{pmatrix},\quad e_2=\begin{pmatrix}0 & 1\\ -p & 0\end{pmatrix},\quad e_3=\begin{pmatrix}0 & \sqrt{r}\\ p\sqrt{r} & 0\end{pmatrix}.$$

Let $\mathfrak{p}|p$ be a prime of $\mathcal{O}_L$ dividing p. Via the identifications in Proposition 3, this is also a basis for Λ_R over $\mathcal{O}_{L_\mathfrak{p}}$ and we have

$$N(xe_1+ye_2+ze_3)=-rx^2+py^2-prz^2,\qquad x,y,z\in\mathcal{O}_{L_\mathfrak{p}}.$$

An application of Hensel's lemma shows that since $p\neq 2$ and is unramified in L, m is represented by $-rx^2+py^2-prz^2$ over $\mathcal{O}_{L_\mathfrak{p}}$ if and only if m is represented by $-rx^2$ over $\mathcal{O}_{L_\mathfrak{p}}$. This, in turn, is equivalent to $-m/r$ being a square modulo $\mathfrak{p}$. Now, $\left(\frac{r}{\mathfrak{p}}\right)=(-1)^{f(\mathfrak{p}/p)}$ so m is representable if and only if $\left(\frac{-m}{\mathfrak{p}}\right)=(-1)^{f(\mathfrak{p}/p)}$. On the other hand, for $p\neq 2$ and unramified in K, we have $\left(\frac{-m}{\mathfrak{p}}\right)=(-1)^{f(\mathfrak{P}/\mathfrak{p})+1}$ for one (or any) prime $\mathfrak{P}|\mathfrak{p}$. We conclude that m is representable locally at a place $\mathfrak{p}|p$ if and only if $f(\mathfrak{P}/\mathfrak{p})+f(\mathfrak{p}/p)$ is odd for all $\mathfrak{P}|\mathfrak{p}$.

Case II b: $p=2$ In this case we write $\mathbb{Z}_4=\mathbb{Z}_2[x]/(x^2+x+1)$. The form N is now given by

$$N\left(\begin{pmatrix}\alpha-\alpha^\sigma & 2\beta\\ -2p\beta^\sigma & \alpha^\sigma-\alpha\end{pmatrix}\right)=-(\alpha-\alpha^\sigma)^2+8\beta\beta^\sigma=3b^2+8\beta\beta^\sigma,\qquad \alpha=a+bx,\ a,b\in\mathbb{Z}_2,\ \beta\in\mathbb{Z}_4.$$

This is a ternary quadratic form over $\mathbb{Z}_2$ and we want to find the conditions under which

$$m=3b^2+8\beta\beta^\sigma,\qquad b\in\mathcal{O}_{L_\mathfrak{p}},\beta\in\mathbb{Z}_4\otimes_{\mathbb{Z}_2}\mathcal{O}_{L_\mathfrak{p}}.$$

We first use Hensel's Lemma mod $\mathfrak{p}^3$ (see for example [Lan, Ch II, §2]). Since $\mathfrak{p}$ is unramified, $m\not\equiv 0 \pmod{\mathfrak{p}}$ and one concludes that m is represented by N if and only if $m=3b^2$, $b\in\mathcal{O}_{L_\mathfrak{p}}$, and that holds if and only if $m=3b^2 \pmod{\mathfrak{p}^3}$. Equivalently, $3m$ is a quadratic residue modulo $\mathfrak{p}^3$.

3.1. **Scholium.** Condition (2) of Theorem A gives a necessary condition for superspecial reduction of the elements in $\mathscr{S}(K)$. This condition should be compared with the results obtained in [Gor]. In fact, what our calculations show is that if K has "large enough" discriminant relative to p then the condition given in Part (2) is also sufficient for having superspecial reduction. Indeed, by these calculations, under the condition on the discriminant (which is not effective), one concludes that there is at least one abelian variety A with CM by $\mathcal{O}_K$ in characteristic zero having superspecial reduction modulo all primes above p. Since $\mathrm{Hom}(A,B)$ for two abelian varieties with CM by $\mathcal{O}_K$ always contains an element of degree prime to p, any abelian variety with CM by $\mathcal{O}_K$ will have superspecial reduction. The condition on "large enough" discriminant can in fact be removed; one knows that when a genus of $\mathcal{O}_L$-integral positive definite quadratic forms represents an element $m\in\mathcal{O}_L$ everywhere locally then *some* form in the genus will represent m globally. See [Han, §2] and the references therein.

4. Proof of Theorem B.

There is a unique superspecial surface over $\overline{\mathbb{F}}_p$, which can be taken to be $E_1 \times E_2$ for any choice of supersingular elliptic curves E_i. Elements of $\mathscr{SS}(A)$ are distinguished by their principal polarization (up to isomorphism). Those, by a result going back to A. Weil, are given by the algebraic equivalence classes of divisors that are either two elliptic curves crossing transversely at their origin, or a non-singular curve of genus two (all up to automorphisms of the abelian variety). There is another description.

Let $A = E \times E$, where E is supersingular elliptic curve. Let $\lambda : A \longrightarrow A^\vee$ be any principal polarization. Recall that the Rosati involution on $\mathrm{End}(A)$, $f \mapsto f^\lambda$, is defined as

$$f^\lambda = \lambda^{-1} f^\vee \lambda,$$

where $f^\vee : A^\vee \longrightarrow A^\vee$ is the dual homomorphism. The map from the Neron-Severi group, NS(A),

$$NS(A) \longrightarrow \mathrm{End}(A), \quad \mu \mapsto \lambda^{-1}\mu,$$

identifies $NS(A)$ with the λ-symmetric elements of $\mathrm{End}(A)$; the polarizations correspond to the λ-totally positive elements under this identification (cf. [Mum, pp. 189-190, 208-210], [IKO, §2.2]). If we choose the product polarization λ_0, coming from the canonical identification of E with $E^\vee$, and $\mathcal{O} = \mathrm{End}(E)$, then the principal polarizations of A are the elements

$$\left\{ \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix} : s,t \in \mathbb{Z}, s,t > 0, r \in \mathcal{O}, st - rr^\vee = 1 \right\}.$$

We first consider a particular case. We take $A = E^2$ with the canonical polarization λ_0. We then want to show that there is an embedding of $\mathcal{O}_L$ into the matrices

$$\Pi(\lambda_0) := \left\{ \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix} : s,t \in \mathbb{Z}, r \in \mathcal{O} \right\},$$

if the discriminant d_L of L is large enough (these are the symmetric matrices with respect to the polarization we picked). Let $\Pi^0(\lambda_0) = \{M \in \Pi(\lambda_0) : \mathrm{Tr}(M) = 0\}$ and let $\Lambda(\lambda_0) = \Pi^0(\lambda_0) \cap (\mathbb{Z} + 2\Pi(\lambda_0))$. This is a rank 5 lattice that can be described explicitly:

$$\Lambda(\lambda_0) = \left\{ \begin{pmatrix} a & 2r \\ 2r^\vee & -a \end{pmatrix} : a \in \mathbb{Z}, r \in \mathcal{O} \right\}.$$

As in §3, one checks that to give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda_0)$ is equivalent to the quintic quadratic form q_{λ_0} given by $a^2 + 4rr^\vee$ representing d_L on $\Lambda(\lambda_0)$. Provided $d_L \gg 0$, this follows from the fact that the quaternary quadratic form $rr^\vee$ on $\mathcal{O}$, a maximal order in $B_{p,\infty}$, represents any large enough integer.

The general case. For every other polarization λ we associate a rank 5 lattice $\Lambda(\lambda)$ with a quadratic form q_λ that will represent d_L if and only if $\mathcal{O}_L$ embeds in the lattice $\Pi(\lambda)$ of λ-symmetric elements of $\mathrm{End}(E^2)$. To show that q_λ represents sufficiently large primitive discriminants, we need to show that there are no local obstructions, for which we shall argue that locally the quintic quadratic modules $(\Lambda(\lambda), q_\lambda)$ and $(\Lambda(\lambda_0), q_{\lambda_0})$ are isomorphic.

Take a matrix $M = \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix}$ defining a principal polarization λ. For any matrix $C = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in M_2(B_{p,\infty})$ we let $C^\vee = \begin{pmatrix} x^\vee & w^\vee \\ y^\vee & z^\vee \end{pmatrix}$. Denote the Rosati involution defined by λ as $N \mapsto N^\lambda$. Then $N^\lambda = M^{-1}N^\vee M$. Let

$$\Pi(\lambda) = \{N \in M_2(\mathcal{O}) : N^\lambda = N\}.$$

By what we said above, the lattice $\Pi(\lambda)$ is isomorphic to $NS(A)$ and so is a rank 6 lattice. We can view $\Pi(\lambda)$ as $\Pi(\lambda) \otimes \mathbb{Q} \cap M_2(\mathcal{O})$. We provide another description of $\Pi(\lambda)$. One may write $M = H^\vee H$

for a suitable $H \in M_2(B_{p,\infty})$ (see [E, Prop. 4.2]). Consider the automorphism of the algebra $M_2(B_{p,\infty})$ given by $N \mapsto H^{-1}NH$. We also denote this by

$$N \mapsto \phi_H(N) = H^{-1}NH.$$

If $N^\vee = N$, i.e. $N \in \Pi(\lambda_0)$, then using the formula $(C_1C_2)^\vee = C_2^\vee C_1^\vee$, one finds that

$$M^{-1}(H^{-1}NH)^\vee M = H^{-1}(H^\vee)^{-1}H^\vee N^\vee (H^{-1})^\vee H^\vee H = H^{-1}NH.$$

That is, $\phi_H(N) = H^{-1}NH$ is an element of $\Pi(\lambda) \otimes \mathbb{Q}$. We find that the rank 6 lattice $\Pi(\lambda)$ is given by

$$\Pi(\lambda) = \phi_H(\Pi(\lambda_0) \otimes \mathbb{Q}) \cap M_2(\mathcal{O}),$$

and so we define a rank 5 lattice

$$\Pi^0(\lambda) = \phi_H(\Pi^0(\lambda_0) \otimes \mathbb{Q}) \cap M_2(\mathcal{O}),$$

and a slightly smaller rank 5 lattice

$$\Lambda(\lambda) = \Pi^0(\lambda) \cap (\mathbb{Z} + 2\Pi(\lambda)).$$

The definition of these lattices is independent of the choice of H such that $M = H^\vee H$. To see that, one first reduces to the case of $M = I$, the identity matrix, so that H satisfies $I = H^\vee H$, i.e. is a rational automorphism of the polarization λ_0. We remark, though this is not needed for our argument, that for any H one has $H^{-1} = (H^\vee H)^{-1}H^\vee$, and for $\vee$-symmetric matrices $\left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right)$ the inverse is given by the usual formula $\frac{1}{x_{11}x_{22}-x_{12}x_{21}} \left(\begin{smallmatrix} x_{22} & -x_{12} \\ -x_{21} & x_{11} \end{smallmatrix}\right)$. The lattice $\Pi(\lambda) \otimes \mathbb{Q}$, according to the definition, now consists of matrices $H^{-1}NH = H^\vee NH$ for which $N^\vee = N$, but it is easy to see that these are again just the $\vee$-symmetric matrices. That is, $\Pi(\lambda)$ is well-defined under our procedure. Next we consider $\Pi^0(\lambda_0)$. Remark that under the ℓ-adic representation on $T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, $j : B_{p,\infty} \hookrightarrow M_2(\mathbb{Q}_\ell)$, we have $\mathrm{Tr}(x) = \mathrm{Tr}(j(x))$. On the other hand, $B_{p,\infty}$, being a finite dimensional $\mathbb{Q}$-algebra, has an intrinsic trace Tr' coming from the left regular representation on itself, and one has $\mathrm{Tr}' = 2\mathrm{Tr}$. Using this it is not hard to see, making use of the ℓ-adic representation, that the intrinsic trace Tr' of an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(B_{p,\infty})$ is just $4\mathrm{Tr}(a) + 4\mathrm{Tr}(d)$. We conclude that the function $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \mathrm{Tr}(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) := \mathrm{Tr}(a) + \mathrm{Tr}(d)$ is invariant under conjugation because Tr' obviously is. Since $\Pi^0(\lambda_0)$ can be described as the $\vee$-symmetric matrices N with $\mathrm{Tr}(N) = 0$, we conclude that its definition is indeed independent of the choice of H, i.e. $\phi_H(\Pi^0(\lambda_0)) = \Pi^0(\lambda_0)$ if $H^\vee H = I$. Note that this argument also gives a more natural definition of the lattice $\Pi^0(\lambda)$ as the integral λ-symmetric matrices of Tr equal to zero and our ad hoc definition is just more convenient for the purpose of our proof.

Lemma 4. *Let $L = \mathbb{Q}(\sqrt{D})$, $D > 0$ square-free, be a real quadratic field with discriminant d_L.*

1. *To give an embedding of L into $\Pi(\lambda) \otimes \mathbb{Q}$ is equivalent to giving an element C of $\Pi^0(\lambda) \otimes \mathbb{Q}$ whose degree as a rational endomorphism is $\deg C = D^2$.*
2. *To give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda)$ is equivalent to giving an element of $\Lambda(\lambda)$ whose degree as an endomorphism is d_L^2.*
3. *Define*
$$q_\lambda : \Lambda(\lambda) \longrightarrow \mathbb{Z}, \qquad q_\lambda(C) = \sqrt{\deg(C)}.$$
The function q_λ is a quintic integral positive definite quadratic form and to give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda)$ is equivalent to representing $-d_L$ by q_λ.

Proof. The whole issue is to map $\sqrt{D}$ to an element $C \in \Pi(\lambda) \otimes \mathbb{Q}$ that will satisfy $C^2 = DI_2$. Composing with ϕ_H^{-1}, one verifies that the condition is that $\mathrm{Tr}(C_1) = 0$ and $\det(C_1) = -D$, where $C_1 = \phi_H^{-1}(C)$ (writing the condition in $\Pi(\lambda) \otimes \mathbb{Q}$ is more complicated; see §4.1). However, for matrices $C_1 = \begin{pmatrix} s & r \\ r^\vee & -s \end{pmatrix}$ we have that $\deg(C_1)^2 = \deg(C_1^2) = \deg \begin{pmatrix} s^2 + rr^\vee & 0 \\ 0 & s^2 + rr^\vee \end{pmatrix} = (s^2 + rr^\vee)^4 = \det(C_1)^4$ and so $\deg(C_1) =$

D^2. However, we have $\deg(C_1) = \deg(C)$ (for the natural extension of the degree map to rational isogenies). Note that this implies that the map $L \longrightarrow \Pi(\lambda) \otimes \mathbb{Q}$ gives a map $\mathbb{Z}[\sqrt{D}] \longrightarrow \Pi(\lambda)$ if and only if $C \in \Pi^0(\lambda)$ and $\deg(C) = D^2$.

One now considers the conditions that actually guarantee that $\sqrt{D}$, or $\frac{1+\sqrt{D}}{2}$ (as the case may be), are in $M_2(\mathcal{O})$. The second part follows.

On $\Pi^0(\lambda_0)$ we have $q_{\lambda_0}\begin{pmatrix} s & r \\ r^\vee & -s \end{pmatrix} = s^2 + rr^\vee$, which is visibly a quintic positive definite quadratic form. Since $q_\lambda(C) = q_{\lambda_0}(\phi_H^{-1}(C))$ on $\Phi_H(\Pi^0(\lambda))$ it follows that it too is a quintic positive definite rational quadratic form. The identity $q_\lambda(C) = \sqrt{\deg(C)}$ implies that q_λ is in fact integral. □

According to Lemma 2.4 of [IKO], given a matrix $M \in \mathrm{GL}_2(\mathcal{O})$ and a prime q we can find a matrix $H = H(q) \in \mathrm{GL}_2(\mathcal{O}_q)$ such that $M = H^\vee H$. That means that locally the lattices $\Lambda(\lambda)$ and $\Lambda(\lambda_0)$ are conjugate by the map ϕ_H. It follows from our definitions that the quadratic modules $(\Lambda(\lambda), q_\lambda)$ and $(\Lambda(\lambda_0), q_{\lambda_0})$ are in the same genus. Therefore, verifying the local representability conditions for q_λ reduces to the case of q_{λ_0} which was already considered.

4.1. **Scholium.** One can give another explicit description of the lattices $\Lambda(\lambda)$ and the conditions for embedding $\mathcal{O}_L$ in them. For simplicity we only describe $\Pi(\lambda)$ and the conditions for embedding $\mathbb{Z}[\sqrt{D}]$ in it. Let $M = \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix}$ define the principal polarization λ. The elements of $\Pi(\lambda)$ are the matrices $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \alpha, \beta, \gamma, \delta \in \mathcal{O}$ such that

$$s\alpha + r\gamma \in \mathbb{Z}, \quad r^\vee\beta + t\delta \in \mathbb{Z}, \quad \alpha^\vee r + \gamma^\vee t = s\beta + r\delta. \tag{4.1}$$

The conditions for $N^2 = D \cdot I_2$ are

$$\alpha\beta = -\beta\delta, \quad \gamma\alpha = -\delta\gamma \tag{4.2}$$

and $\alpha^2 + \beta\gamma = \delta^2 + \gamma\beta = D$, which reduce given (4.2) to one condition:

$$\alpha^2 + \beta\gamma = D. \tag{4.3}$$

As noted, the matrices satisfying (4.1) are a rank 6 lattice over $\mathbb{Z}$. In fact the last equation can be written in the form

$$\alpha^2 + \beta\gamma = \frac{\beta\beta^\vee + (m')^2}{t^2},$$

where $m' = r^\vee\beta + t\delta \in \mathbb{Z}$.

References

[Cha] Chai, C.-L.: Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli. Invent. Math. 121 (1995), no. 3, 439–479.

[Cog] Cogdell, J. W.: On sums of three squares. Les XXIIémes Journées Arithmétiques (Lille, 2001). J. Théor. Nombres Bordeaux 15 (2003), no. 1, 33–44.

[DSG] de Shalit, E.; Goren, E. Z.: On special values of theta functions of genus two. Ann. Inst. Fourier (Grenoble) 47 (1997), no. 3, 775–799.

[D] Duke, W.: Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math. 92 (1988), 73-90.

[E] Ekedahl, T.: On supersingular curves and abelian varieties. Math. Scand. 60 (1987), no. 2, 151–178.

[EOY] Elkies, N.; Ono, K; Yang, T.: Reduction of CM elliptic curves and modular function congruences. IMRN International Mathematics Research Notices (2005), No. 44, 2695–2707.

[Ghi] Ghitza, A.: Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms. J. Number Theory 106 (2004), no. 2, 345–384.

[Gor] Goren, E. Z.: On certain reduction problems concerning abelian surfaces. Manuscripta Math. 94 (1997), no. 1, 33–43.

[GL] Goren, E. Z.; Lauter, K. E.: Class invariants of quartic CM fields (2004), http://www.arxiv.org/pdf/math.NT/0404378, submitted.

[GN] Goren, E. Z.; Nicole, M.-H.: Superspecial abelian varieties, quaternion algebras and Hilbert modular forms, Manuscript in preparation.

[GO] Goren, E. Z.; Oort, F.: Stratifications of Hilbert modular varieties. J. Algebraic Geom. 9 (2000), no. 1, 111–154.
[GZ] Gross, B. H.; Zagier, D. B.: On singular moduli. J. Reine Angew. Math. 355 (1985), 191–220.
[Han] Hanke, J.: Some recent results about (ternary) quadratic forms. Number theory, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI (2004), 147–164.
[IKO] Ibukiyama, T.; Katsura, T.; Oort, F.: Supersingular curves of genus two and class numbers. Compositio Math. 57 (1986), no. 2, 127–152.
[I] Iwaniec, H.: Fourier coefficients of modular forms of half-integral weight, Invent. Math. 87 (1987), 385-401.
[Lan] Lang, Serge: Algebraic number theory. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.
[Mum] Mumford, D.: Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5 Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970.
[Nic] Nicole, M-H.: Superspecial abelian varieties, theta series and the Jacquet-Langlands correspondence. Doctoral Thesis, McGill University, June 2005.
[Rap] Rapoport, M.: Compactifications de l'espace de modules de Hilbert-Blumenthal. Compositio Math. 36 (1978), no. 3, 255–335.
[Ser] Serre, J-P.: Local Fields. Graduate Texts in Mathematics, 67. Springer, New York, 1979.
[Vig] Vignéras, M.-F.: Arithmétique des algèbres de quaternions. Lecture Notes in Mathematics, 800. Springer, Berlin, 1980.
[WM] Waterhouse, W. C.; Milne, J. S.: Abelian varieties over finite fields. 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), pp. 53–64. Amer. Math. Soc., Providence, R.I., 1971.

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W., Montreal H3A 2K6, QC, Canada.

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA.
E-mail address: goren@math.mcgill.ca; klauter@microsoft.com